JOURNAL OF ALGEBRA 111, 114–132 (1987)

Multigroups

BORIS M. SCHEIN

Department of Mathematical Sciences, University of Arkansas, Fayetteville, Arkansas 72701

Communicated by G. B. Preston

Received March 26, 1985

TO THE MEMORY OF V. V. WAGNER, MY TEACHER

INTRODUCTION

Historically, group theory appeared as the theory of transformation groups. The concept of an abstract group appeared later (cf. [8, 25]) as an abstract notion coinciding (up to isomorphism) with that of transformation group (that is, every transformation group is a group and every abstract group is isomorphic to a transformation group).

A transformation group is a set of transformations of some set, say A, closed under two operations: composition (=superposition) and involution (=inversion) of transformations.

Here "transformation" means a binary relation ϕ on A satisfying the following conditions:

(A) ϕ is everywhere defined, i.e., for every $a \in A$ there exists $a, b \in A$, called an image of a under ϕ, such that $(a, b) \in \phi$ (in other words, the domain of ϕ is A);

(B) ϕ is single-valued, i.e., $(a, b) \in \phi$ and $(a, c) \in \phi$ imply $b = c$ for any $a, b, c \in A$ (in other words, no element of A can have more than one image under ϕ).

A composition of two binary relations ϕ and ψ is a binary relation $\psi \circ \phi$ such that $(a, c) \in \psi \circ \phi$ if and only if $(a, b) \in \phi$ and $(b, c) \in \psi$ for some $b \in A$. If ϕ and ψ are transformations, then this definition of $\psi \circ \phi$ is equivalent to

$$\psi \circ \phi(a) = \psi(\phi(a)), \tag{1}$$

where $\phi(a)$ is, of course, the single image of $a \in A$ under ϕ. The involution is a unary operation which, for every binary relation ϕ, produces the converse relation ϕ^{-1} defined as

$$(a, b) \in \phi^{-1} \Leftrightarrow (b, a) \in \phi \qquad \text{for all} \quad a, b \in A.$$

0021-8693/87 $3.00

If Φ is a group of transformations then for every $\phi \in \Phi$ the converse relation ϕ^{-1} must belong to Φ, so ϕ^{-1} is a transformation, i.e., ϕ^{-1} satisfies the conditions (A) and (B) above. The domain of ϕ^{-1} is the range of ϕ, so (A) holds for ϕ^{-1} exactly when ϕ^{-1} is surjective. Now, (B) holds for ϕ^{-1} exactly when ϕ is injective. Thus, $\phi \in \Phi$ must be a bijection of A onto itself, i.e., Φ consists of permutations of A. Here we consider permutations of the sets which are not necessarily finite. A set Ψ of binary relations closed under composition and involution (and considered relative to these two operations) is called an *involutive semigroup of binary relations*. So transformation groups are precisely involutive semigroups of permutations.

If we omit (A) in the above definition of transformation, we arrive at the so-called *partial transformations* of A. The domain of a partial transformation need not coincide with A (e.g., the domain may be empty). The composition of partial transformations may be defined by (1), where both sides of the equality make or do not make sense simultaneously (this last condition pertains to the fact that if ϕ is a partial transformation and $a \in A$, then the image $\phi(a)$ of a may not exist).

Let Φ be an involutive semigroup of partial transformations. Since, with every ϕ, the converse relation ϕ^{-1} must belong to Φ, we see that ϕ^{-1} must satisfy (B), i.e., ϕ is injective. Thus, Φ is an involutive semigroup of one-to-one partial transformations. In 1952, V. V. Wagner [23] considered such systems and called them *generalized groups* of partial transformations. He defined abstract generalized groups and proved that every generalized group of partial transformations was a generalized group and that every abstract generalized group was isomorphic to a generalized group of partial transformations. In 1954 the same results were obtained by G. B. Preston [9, 10], who coined the term *inverse semigroup* synonymous with "generalized group." Another proof of the Wagner–Preston theorem is given in [14, Theorem 3]. Being considered as algebras with two operations, a binary multiplication and a unary involution, inverse semigroups are precisely the algebras satisfying the identities [15]

$$\begin{gathered}(xy)z = x(yz), \qquad (x^{-1})^{-1} = x, \qquad (xy)^{-1} = y^{-1}x^{-1}, \\ xx^{-1}x = x, \qquad xx^{-1}x^{-1}x = x^{-1}xxx^{-1}.\end{gathered} \tag{2}$$

The algebras which satisfy the first three of these identities are called (abstract) *involutive semigroups*; those which satisfy the first four identities are called **-regular semigroups*, or *semigroups with inverting involution.*

Now, while preserving (A), one may omit condition (B) in the above definition of transformations. Then one arrives at "transformations" which, though not necessarily single-valued, are everywhere defined. We call such binary relations "multitransformations."

Suppose that Φ is an involutive semigroup of multitransformations. For every $\phi \in \Phi$ the converse ϕ^{-1} belongs to Φ, so both the domain and range of ϕ coincide with A. We call such binary relations "multipermutations."

In this paper we characterize involutive semigroups of multipermutations. We find a class of abstract involutive semigroups which, up to isomorphism, coincide with involutive semigroups of multipermutations. We call such systems "multigroups." The term "multigroups" has been used elsewhere in another sense (for "algebras" in which the "product" of two elements did not necessarily have a single value).

So, along with inverse semigroups, multigroups are generalizations of groups. Every group is, of course, an inverse semigroup as well as a multigroup. It turns out that the class of abstract multigroups is wider than that of inverse semigroups: every inverse semigroup is a multigroup (i.e., every inverse semigroup is isomorphic to an involutive semigroup of multipermutations), and we characterize those involutive semigroups of multipermutations which are inverse semigroups. This gives an entirely new representation theorem for inverse semigroups, a theorem which differs from the Wagner–Preston representation theorem. In a sense, this new representation theorem is dual to the Wagner–Preston one.

We also characterize some related algebraic systems. If Φ is a set of binary relations on an underlying set A, then Φ is a set of subsets of $A \times A$. Like every set of subsets, Φ is (partially) ordered by the set-theoretical inclusion. So we may consider ordered semigroups and ordered involutive semigroups of binary relations. To emphasize that the order on our semigroup is not arbitrary, we call such systems *fundamentally* ordered. This term is due to V. V. Wagner [24]. Thus, a *fundamentally ordered involutive semigroup* (f.o.i.s.) of binary relations is any algebraic system of the form $(\Phi; \circ, ^{-1}; \subset)$, where $(\Phi; \circ, ^{-1})$ is an involutive semigroup and $(\Phi; \subset)$ is an inclusion-ordered set of binary relations.

It may happen that Φ is a Boolean algebra relative to $\subset$. Then we may consider systems of the form $(\Phi; \circ, ^{-1}, \bigcap, \bigcup, ', \varnothing, U, \Delta)$, where $(\Phi; \circ, ^{-1})$ is an involutive semigroup of binary relations, $\bigcap$, $\bigcup$, and $'$ are the set-theoretical operations of intersection, union, and complementation, and $\varnothing$, U, Δ are the empty, universal, and identity binary relations, respectively. Such systems are called Tarski relation algebras [22]; their abstract axiomatic characterization was found by R. C. Lyndon [4, 5]. If Φ consists of multipermutations, then the corresponding systems are called *Tarski integral relation algebras*. If Φ is closed under the binary set-theoretical intersection $\bigcap$, we may consider algebras of the form $(\Phi; \circ, ^{-1}, \bigcap, \Delta)$. We call them *Jónsson relation algebras*. Their abstract axiomatic characterization is due to B. Jónsson [3].

Fundamentally ordered involutive semigroups of arbitrary binary relations were characterized in each of the publications [1, 20, 21].

Some results of this paper have been announced by the author previously [17] without proofs.

1. Fundamentally Ordered Multigroups

An *ordered involutive semigroup* is any algebraic system of the form $(S;\cdot,^{-1};\leqslant)$, where $(S;\cdot,^{-1})$ is an involutive semigroup, $(S;\leqslant)$ is a (partially) ordered set, and the order relation $\leqslant$ is stable under both algebraic operations $\cdot$ and $^{-1}$, i.e., $x_1 \leqslant x_2$ and $y_1 \leqslant y_2$ imply $x_1 y_1 \leqslant x_2 y_2$, while $x \leqslant y$ implies $x^{-1} \leqslant y^{-1}$ for all $x, y, x_1, y_1, x_2, y_2 \in S$.

Clearly, every fundamentally ordered involutive semigroup of binary relations is an ordered involutive semigroup.

Theorem 1. *An ordered involutive semigroup is isomorphic to a fundamentally ordered involutive semigroup of multipermutations if and only if the inequality*

$$x \leqslant yy^{-1}x \tag{3}$$

is satisfied for all elements x, y. If our algebraic system contains a multiplicative identity 1, *then* (3) *is equivalent to*

$$1 \leqslant yy^{-1} \qquad \textit{for all} \quad y. \tag{4}$$

Proof. Suppose $(\Phi;\circ,^{-1};\subset)$ is a fundamentally ordered involutive semigroup of multipermutations of an underlying set A. Clearly, for every $\phi \in \Phi$ and every $a \in A$ there exists $b \in A$ such that $(b, a) \in \phi$. Then $(a, a) \in \phi \circ \phi^{-1}$. It follows that for every $\psi \in \Phi$, $\psi \subset \phi \circ \phi^{-1} \circ \psi$, i.e., (3) holds.

Conversely, let $(S;\cdot,^{-1};\leqslant)$ be an ordered involutive semigroup satisfying (3). Without loss of generality we may suppose that the semigroup $(S;\cdot)$ has an identity. Indeed, if $(S;\cdot)$ is a semigroup without identity, we can adjoin a new element 1 to S extending $\cdot$ so that 1 is a multiplicative identity and defining $1^{-1} = 1$, $s \leqslant 1$ if and only if $s = 1$, $1 \leqslant s$ for $s \in S$ if and only if there exists $t \in S$ such that $tt^{-1} \leqslant s$. Clearly, $S^1 = S \cup \{1\}$ is an involutive semigroup under these operations. Now, $\leqslant$ is an order relation on S^1. Indeed, $\leqslant$ is obviously reflexive and antisymmetric, and one can easily see that $\leqslant$ is transitive.

If $1 \leqslant s$ and $tt^{-1} \leqslant s$, then $tt^{-1} = (tt^{-1})^{-1} \leqslant s^{-1}$, i.e., $1^{-1} = 1 \leqslant s^{-1}$.

If $1 \leqslant s$ and $1 \leqslant t$ for some $s, t \in S$, then $uu^{-1} \leqslant s$ and $vv^{-1} \leqslant t$ for some $u, v \in S$. Then $uu^{-1}vv^{-1} \leqslant st$. Using (3) we see that $vv^{-1} \leqslant uu^{-1}vv^{-1} \leqslant st$. Thus $1 \leqslant st$. If $s_1 \leqslant s_2$ for some $s_1, s_2 \in S$, then, by (3), $s_1 \leqslant s_2 \leqslant uu^{-1}s_2 \leqslant ss_2$. Analogously, $s_1 \leqslant s_2 s$. Thus $\leqslant$ is stable under both algebraic operations of S^1. Therefore, S^1 is an ordered involutive semigroup.

Now, S^1 satisfies (3). Indeed, if $y=1$ then (3) is obvious. If $x=1$ then $yy^{-1} \leqslant yy^{-1}$, and so $1 \leqslant yy^{-1}$.

So, without loss of generality, we may suppose that $(S; \cdot)$ has an identity 1.

A subset H of S is called *majorantly saturated* if, for every $s, t \in S$ such that $s \leqslant t$ and $s \in H$, we have $t \in H$. Let M be the set of all majorantly saturated subsets of S. Define a mapping ϕ of S into the set of all binary relations on M as follows: if $s \in S$ and $A, B \in M$, then $(A, B) \in \phi(s)$ if and only if $sA \subset B$ and $s^{-1}B \subset A$. It follows from this definition that $\phi(s^{-1}) = \phi(s)^{-1}$. Suppose that $(A, B) \in \phi(s) \circ \phi(t)$. Then $(A, C) \in \phi(t)$ and $(C, B) \in \phi(s)$ for certain $C \in M$. Thus $tA \subset C$, $t^{-1}C \subset A$, $sC \subset B$, $s^{-1}B \subset C$, and so $stA \subset sC \subset B$, $(st)^{-1}B = t^{-1}s^{-1}B \subset t^{-1}C \subset A$; hence $(A, B) \in \phi(st)$. Conversely, let $(A, B) \in \phi(st)$, i.e., $stA \subset B$ and $t^{-1}s^{-1}B \subset A$. Let C be the least majorantly saturated subset of S which contains both tA and $s^{-1}B$. By its definition, $tA \subset C$ and $s^{-1}B \subset C$. Clearly, $u \in C$ if and only if $v \leqslant u$ for some $v \in tA \cup s^{-1}B$. Consider $t^{-1}C$. If $u \in C$, then $t^{-1}v \leqslant t^{-1}u \in t^{-1}C$. If $v \in tA$, then $v = ta$ for some $a \in A$. Thus $a \leqslant t^{-1}ta = t^{-1}v \leqslant t^{-1}u \in t^{-1}C$. Here we have used (3) for $t^{-1} = y$, $a = x$. Since $A \in M$, we have $t^{-1}u \in A$. If $v \in s^{-1}B$, then $v = s^{-1}b$ for some $b \in B$. Thus $t^{-1}s^{-1}b = t^{-1}v \leqslant t^{-1}u \in t^{-1}C$. However, $t^{-1}s^{-1}b \in A$, since $t^{-1}s^{-1}B \subset A$; hence $t^{-1}u \in A$. Therefore $t^{-1}u \in A$ for all $u \in C$, i.e., $t^{-1}C \subset A$. Analogously, $sC \subset B$. We have proved that $(A, C) \in \phi(t)$ and $(C, B) \in \phi(s)$ for some $C \in M$. Therefore, $(A, B) \in \phi(s) \circ \phi(t)$. In other words, $\phi(s) \circ \phi(t) = \phi(st)$ for all $s, t \in S$.

Now suppose that $s \leqslant t$ for some $s, t \in S$. If $(A, B) \in \phi(s)$, i.e., if $sA \subset B$ and $s^{-1}B \subset A$, then, for every $a \in A$, $sa \leqslant ta$. Since $sa \in B$ and B is majorantly saturated, $ta \in B$. Thus $tA \subset B$. Since $s^{-1} \leqslant t^{-1}$ and $s^{-1}B \subset A$, we have by the same argument that $t^{-1}B \subset A$; whence $(A, B) \in \phi(t)$. Therefore $\phi(s) \subset \phi(t)$.

Conversely, suppose that $\phi(s) \subset \phi(t)$ for some $s, t \in S$. Let $H_1 = \{u \in S\colon 1 \leqslant u\}$, and $H_2 = \{v \in S\colon s \leqslant v\}$. Then $H_1, H_2 \in M$. Obviously, $sH_1 \subset H_2$. Suppose that $v \in H_2$, i.e., $s \leqslant v$. Then $s^{-1}s \leqslant s^{-1}v$. By (3), $1 \leqslant s^{-1}s1$, so $1 \leqslant s^{-1}v$ and $s^{-1}v \in H$. Thus $s^{-1}H_2 \subset H_1$. Therefore, $(H_1, H_2) \in \phi(s) \subset \phi(t)$. It follows that $t = t1 \in tH_1 \subset H_2$, i.e., $s \leqslant t$. Thus $s \leqslant t$ if and only if $\phi(s) \subset \phi(t)$. In particular, if $\phi(s) = \phi(t)$, then $\phi(s) \subset \phi(t)$ and $\phi(t) \subset \phi(s)$, hence $s \leqslant t$ and $t \leqslant s$, thus $s = t$. It follows that ϕ is an isomorphism of $(S; \cdot, ^{-1}; \leqslant)$ onto a fundamentally ordered involutive semigroup of multipermutations.

If $(S; \cdot)$ is a semigroup with 1, then (3) implies (4) when $x = 1$ is substituted in (3). Conversely, if (3) is multiplied by x on the left, we get (4), so (3) and (4) are equivalent. This completes the proof of our theorem.

We assumed ϕ to be a multiplicative homomorphism if $\phi(st) = \phi(s) \circ \phi(t)$ for all $s, t \in S$. In our previous publications (e.g., in [16]) we used $\phi(st) = \phi(t) \circ \phi(s)$ instead. Had we used this latter condition in this paper, we had to define $(A, B) \in \phi(s)$ if and only if $As \subset B$ and $Bs^{-1} \subset A$ instead of our definition of $\phi(s)$.

2. Axiomatization of Multigroups

THEOREM 2. *An involutive semigroup S is a multigroup (i.e., S is isomorphic to an involutive semigroup of multipermutations of a set) if and only if, for every $n > 1$, it satisfies the following condition I_n:*

$$\begin{aligned} x_1 y_1 y_1^{-1} z_1 &= x_2 z_2, \\ x_2 y_2 y_2^{-1} z_2 &= x_3 z_3, \\ &\cdots\cdots \\ x_{n-1} y_{n-1} y_{n-1}^{-1} z_{n-1} &= x_n z_n, \\ x_n y_n y_n^{-1} z_n &= x_1 z_1 \text{ imply } x_1 z_1 = x_2 z_2 \end{aligned} \tag{5}$$

for all $x_i, y_i, z_i \in S^1$, $1 \leqslant i \leqslant n$.

Proof. First of all, we will elucidate the meaning of I_n. To this end we introduce a binary relation ρ_n on S for every $n > 1$ as follows: for $s, t \in S$ we define $(s, t) \in \rho_n$ if and only if $s = t$ or there exist $x_i, y_i, z_i \in S^1$, $1 \leqslant i \leqslant n$, such that $s = x_1 z_1$, $t = x_n z_n$ and the following equalities hold:

$$\begin{aligned} x_1 y_1 y_1^{-1} z_1 &= x_2 z_2, \\ x_2 y_2 y_2^{-1} z_2 &= x_3 z_3, \\ &\cdots\cdots \\ x_{n-1} y_{n-1} y_{n-1}^{-1} z_{n-1} &= x_n z_n. \end{aligned}$$

Following are some of the properties of ρ_n:

Property 1. If $n < m$, then $\rho_n \subset \rho_m$.

Proof. Let $(s, t) \in \rho_n$. Choose x_i, y_i, z_i as in the definition of ρ_n. Let $x_{n+1} = x_n$, $z_{n+1} = z_n$, and let y_n be an empty symbol (equivalenty, y_n is the identity element of S^1). Then $x_n y_n y_n^{-1} z_n = x_{n+1} z_{n+1} = t$, hence $(s, t) \in \rho_{n+1}$. Thus $\rho_n \subset \rho_{n+1}$ for every n. Property 1 follows immediately.

Property 2. For all m and n the following inclusion holds: $\rho_m \circ \rho_n \subset \rho_{m+n-1}$.

Proof. Let $(s, t) \in \rho_n$ and $(t, u) \in \rho_m$. If $s = t$ or $t = u$, we apply Property 1. Let $s = x_1 z_1$, $t = x_n z_n$, $x_i y_i y_i^{-1} z = x_{i+1} z_{i+1}$ for $1 \leqslant i \leqslant n-1$. Also let $t = \bar{x}_1 \bar{z}_1$, $u = \bar{x}_m \bar{z}_m$, and $\bar{x}_j \bar{y}_j \bar{y}_j^{-1} \bar{z}_j = \bar{x}_{j+1} \bar{z}_{j+1}$ for $1 \leqslant j \leqslant m-1$. Without loss of generality we may assume that $x_n = \bar{x}_1$ and $z_n = \bar{z}_1$, because $\bar{x}_1 \bar{z}_1 = t = x_n z_n$. Now assume that $x_{n+j-1} = \bar{x}_j, y_{n+j-1} = \bar{y}_j$, and $z_{n+j-1} = \bar{z}_j$ for all $1 \leqslant j \leqslant m-1$. Then $x_1 z_1 = s$, $x_{m+n-1} z_{m+n-1} = \bar{x}_m \bar{z}_m = u$, and $x_i y_i y_i^{-1} z_i = x_{i+1} z_{i+1}$ for $1 \leqslant i \leqslant m+n-2$. Thus, $(s, u) \in \rho_{m+n-1}$.

Let $\rho = \bigcup \{\rho_n : n > 1\}$. By Property 2 this relation is transitive. It is also reflexive. Thus ρ is a quasi-order relation on S. For every n and for any s, t, $u \in S$, it is easily seen that $(s, t) \in \rho_n$ implies $(su, tu) \in \rho_n$ and $(us, ut) \in \rho_n$. To prove that $(su, tu) \in \rho_n$ it suffices to replace all z_i occurring in the definition of $(s, t) \in \rho_n$ by $z_i u$; to prove $(us, ut) \in \rho_n$ one replaces all x_i by ux_i. It follows that $(s, t) \in \rho$ implies $(su, tu) \in \rho$ and $(us, ut) \in \rho$. Since ρ is a quasi-order relation, it follows that ρ is stable under multiplication of S. If we replace all x_i by z_i^{-1}, and all z_i by x_i^{-1} in the definition of $(s, t) \in \rho_n$, we obtain that $(s, t) \in \rho_n$ implies $(s^{-1}, t^{-1}) \in \rho_n$. It follows that $(s, t) \in \rho \Rightarrow (s^{-1}, t^{-1}) \in \rho$, i.e., ρ is stable under involution. Finally, assuming $x_1 = x_2 = 1$, $y_1 = y$, $z_1 = x$, $z_2 = yy^{-1}x$, we obtain $(x, yy^{-1}x) \in \rho_2$ for any x, $y \in S$. Therefore, $(x, yy^{-1}x) \in \rho$.

Property 3. ρ is the least element (with respect to set-theoretical inclusion) of the set of all stable quasi-order relations satisfying (3) on $(S; \cdot, ^{-1})$.

Proof. Let τ be a stable quasi-order relation on S and let $(x, yy^{-1}x) \in \tau$ for all x, $y \in S$ (i.e., τ satisfies (3)). Suppose that $(s, t) \in \rho_n$, i.e., $s = x_1 z_1$, $t = x_n z_n$, and $x_i y_i y_i^{-1} z_1 = x_{i+1} z_{i+1}$ for suitable x_i, y_i, z_i. Then $(z_i, y_i y_i^{-1} z_i) \in \tau$ by (3) and, since τ is stable relative to multiplication, $\langle x_i z_i, x_i y_i y_i^{-1} z_i) \in \tau$. Therefore, $(x_i z_i, x_{i+1} z_{i+1}) \in \tau$ for all i. Since τ is transitive, we obtain $(x_1 z_1, x_n z_n) \in \tau$, i.e., $(s, t) \in \tau$. Thus, $\rho_n \subset \tau$. Since this is true for all n, we obtain $\rho \subset \tau$.

Property 4. An involutive semigroup is a multigroup if and only if the relation ρ on it is anti-symmetric.

Proof. Let S be a multigroup. There exists an isomorphism ψ of S onto an involutive semigroup of multipermutations of a set. Define: $(s, t) \in \tau \Leftrightarrow \psi(s) \subset \psi(t)$ for any $s, t \in S$. Then $(S; \cdot, ^{-1}, \tau)$ is an ordered involutive semigroup and ψ is its isomorphism onto an inclusion-ordered involutive semigroup of multipermutations. By Theorem 1, τ is an order relation satisfying (3). By Property 3, $\rho \subset \tau$. Since τ is anti-symmetric, ρ is also. Conversely, if ρ is anti-symmetric, then it is an order relation and $(S; \cdot, ^{-1}, \rho)$ satisfies the conditions of Theorem 1. Therefore, $(S; \cdot, ^{-1})$ is isomorphic to an involutive semigroup of permutations, i.e., it is a multigroup. Anti-symmetry of ρ means that $\rho \cap \rho^{-1} \subset \Delta_S$, where Δ_S is the equality relation on S. Equivalently,

$$\rho_m \cap \rho_n^{-1} \subset \Delta_S \qquad \text{for all } m, n. \tag{6}$$

Consider (6). Let $(s, t) \in \rho_m \cap \rho_n^{-1}$. This means that $(s, t) \in \rho_m$ and $(t, s) \in \rho_n$. Thus, $s = x_1 z_1$, $t = x_m z_m$, $x_i y_i y_i^{-1} z_i = x_{i+1} z_{i+1}^{-1}$ for $1 \leqslant i \leqslant m-1$ and $t = \bar{x}_1 \bar{z}_1$, $s = \bar{x}_n \bar{z}_n$, $\bar{x}_j \bar{y}_j \bar{y}_j^{-1} \bar{z}_j = \bar{x}_{j+1} \bar{z}_{j+1}$ for $1 \leqslant j \leqslant n-1$. Without loss of generality we may assume that $\bar{x}_1 = x_m$ and $\bar{z}_1 = z_m$. Also, assume that $x_{m+j-1} = \bar{x}_j$, $y_{m+j-1} = \bar{y}_j$, $z_{m+j-1} = \bar{z}_j$ for $1 \leqslant j \leqslant n-1$. Then the condition $\rho_m \cap \rho_n^{-1} \subset \Delta_S$ can be written in the equivalent form

$$
\begin{gathered}
x_1 y_1 y_1^{-1} z_1 = x_2 z_2, \\
x_2 y_2 y_2^{-1} z_2 = x_3 z_3, \\
\cdots\cdots\cdots\cdots \\
x_{m+n-2} y_{m+n-2} y_{m+n-2}^{-1} z_{m+n-2} = x_{m+n-1} z_{m+n-1}, \\
x_{m+n-1} y_{m+n-1} y_{m+n-1}^{-1} z_{m+n-1} = x_1 z_1 \quad \Rightarrow \quad x_1 z_1 = x_m z_m.
\end{gathered} \tag{7}
$$

Next consider condition I_n. Clearly, the antecedent of I_n implies not only that $x_1 z_1 = x_2 z_2$ but also that $x_1 z_1 = x_2 z_2 = x_3 z_3 = \cdots = x_n z_n$. Indeed, permuting the rows in the antecedent of I_n cyclically, we obtain

$$
\begin{gathered}
x_2 y_2 y_2^{-1} z_2 = x_3 z_3, \\
\cdots\cdots\cdots\cdots \\
x_n y_n y_n^{-1} z_n = x_1 z_1, \\
x_1 y_1 y_1^{-1} z_1 = x_2 z_2.
\end{gathered}
$$

Applying I_n we obtain $x_2 z_2 = x_3 z_3$. Analogously we obtain $x_3 z_3 = x_4 z_4$, and so on. Thus, (7) follows from I_{m+n-1} in which some variables are allowed to be empty symbols.

Hence, S is a multigroup if and only if it satisfies all the conditions I_n in which y_i can be empty symbols. However, if y_i's are empty in m cases precisely in I_n, then I_n is equivalent to I_{n-m} where the y_i are not empty symbols. Indeed, if y_k is an empty symbol in I_n then, without loss of generality, we may assume that $x_k = x_{k+1}$, $z_k = z_{k+1}$, and we can omit the kth row of the antecedent of I_n. Omitting all k rows which contain empty y_i's, we arrive at an antecedent of I_{n-m} in which no y_i is an empty symbol, and our formula I_n will turn into I_{n-m}. Thus, S is a multigroup precisely when it satisfies all conditions I_n. This completes the proof of Theorem 2.

This theorem gives an axiomatic characterization of multigroups. The characterization is an infinite set of elementary axioms (here "elementary" means a formula of the first-order predicate calculus). These axioms are not identities. Two questions arise:

(a) Do multigroups form a variety of algebras (i.e., can they be characterized by a set of identities)?

(b) Can multigroups be characterized by a finite system of elementary axioms?

We will provide negative answers to both questions.

THEOREM 3. *The class of all multigroups is not a variety.*

Proof. We will prove that a homomorphic image of a multigroup need not be a multigroup. As a first step we consider free involutive semigroups. Almost obviously, a free involutive semigroup over a set X of free generators has the following structure.

Let $X^{-1} = \{x^{-1} : x \in X\}$ and suppose that $X \cap X^{-1} = \varnothing$. Consider the free semigroup F of all nonempty words in the alphabet $Y = X \cap X^{-1}$. Define the involution $^{-1}$ in F as follows: if $w = y_1 y_2 \cdots y_n \in F$, $y_i \in Y$, then $w^{-1} = y_n^{-1} \cdots y_2^{-1} y_1^{-1}$, where, if $y_i \in X$, then $y_i^{-1} \in X^{-1}$ and if $y_i \in X^{-1}$, i.e., if $y_i = x^{-1}$ for some $x \in X$, then $y_i^{-1} = x$. Quite obviously, F is an involutive semigroup. It is easy to see that F is free.

Now suppose that the antecedent of I_n holds in F, i.e.,

$$a_1 b_1 b_1^{-1} c_1 = a_2 c_2,$$

$$a_2 b_2 b_2^{-1} c_2 = a_3 c_3,$$

$$\cdots\cdots\cdots\cdots$$

$$a_n b_n b_n^{-1} c_n = a_1 c_1, \qquad \text{for some } a_i, b_i, c_i \in F.$$

Comparing the lengths of the words which constitute the left- and right-hand sides of these equalities we see that $b_i b_i^{-1}$ must always have length 0, i.e., b_i is the empty word (which is interpreted as the identity of F^1). So $a_1 b_1 = a_2 b_2 = \cdots = a_n b_n$ and I_n holds.

Thus, any free involutive semigroup is a multigroup, since it satisfies I_n for all $n > 1$.

Next we construct an involutive semigroup which is not a multigroup.

Let Z_3 be a cyclic group of order 3 with the set of elements $\{0, 1, 2\}$ and an additively written operation $+$. For every $z \in Z_3$ define $z^{-1} = z$. Then Z_3 is an involutive semigroup. Suppose that $z_1 = z_2 = 0$, $x_1 = y_2 = 1$, $x_2 = y_1 = 2$. Then $x_1 + y_1 + y_1^{-1} + z_1 = 2 = x_2 + z_2$, $x_2 + y_2 + y_2^{-1} + z_2 = 1 = x_1 + z_1$. However, $x_1 + z_1 \neq x_2 + z_2$, and so Z_3 does not satisfy I_2. Thus Z_3 is not a multigroup. As an involutive semigroup, Z_3 is a homomorphic image of a free involutive semigroup (actually Z_3 is a homomorphic image of a free involutive semigroup with a single generator).

It follows that the class of all multigroups is not a variety, because it is not closed under homomorphisms. Theorem 3 is proved.

THEOREM 4. *The class of all multigroups is not finitely axiomatizable, i.e., it cannot be characterized by any finite system of elementary axioms.*

Proof. Suppose an involutive semigroup satisfies I_n. Let the antecedent of I_{n-1} be satisfied for some $x_i, y_i, z_i \in S^1$, $1 \leqslant i \leqslant n-1$. Put $x_n = x_{n-1}$, $y_n = 1$, $z_n = z_{n-1}$. Then the antecedent of I_n is satisfied, hence $x_1 z_1 = x_2 z_2$. Thus S satisfies I_{n-1}.

We have proved that I_n implies I_{n-1} for all $n > 2$. Next we will prove that I_{n-1} does not imply I_n.

Consider a finitely presented involutive semigroup S_n. It is generated by the elements x_i, y_i, z_i, $1 \leqslant i \leqslant n+1$; its defining relations are all the equalities at the antecedent of I_{n+1}. Since I_{n+1} is not trivial (i.e., there exist involutive semigroups which do not satisfy I_{n+1}), S_n does not satisfy I_{n+1}. We are going to prove that S_n satisfies I_k for $k \leqslant n$. Elements of S_n are classes of equivalent words. We include the empty word among them; it represents the identity of S_n.

In each element of S_n (i.e., in each class of equivalent words) there is a unique *canonical* word. Suppose a is a word. Replacing all occurrences of $x_i y_i y_i^{-1} z_i$ $[z_i^{-1} y_i y_i^{-1} x_i^{-1}]$ in a by $x_{i+1} z_{i+1}$ $[z_{i+1}^{-1} x_{i+1}^{-1}]$ (or by $x_1 z_1$ $[z_1^{-1} x_1^{-1}]$ in case $i = n+1$) we get a word $\bar{a}$ which is called the *canonical* form of a. Clearly, the canonical form is uniquely determined, it does not depend on particular order in which we replace some subwords by the other ones in a. Clearly, both a and $\bar{a}$ represent a same element of S_n. Moreover, we see from the external form of defining relations of S_n that, for two words a and b, $a \equiv b \Leftrightarrow \bar{a} = \bar{b}$. Here $\equiv$ denotes the equivalence and $=$ the equality (coincidence) of words. So each class of equivalent words contains a single word which is in canonical form. This word is called the *canonical word.* Without loss of generality we will consider S_n as consisting of canonical words with the multiplication $a \cdot b = \overline{ab}$ for all $a, b \in S_n$. Here ab is the concatenation (juxtaposition) of a and b. Clearly, if $a \in S_n$ then $a^{-1} \in S_n$, this gives us the involution operation in S_n.

Suppose that not all of the axioms I_k, $k \leqslant n$, hold in S_n. Choose the minimal $m \leqslant n$ such that I_m does not hold in S_n. That means that there exist canonical words a_i, b_i, c_i from S_n, $1 \leqslant i \leqslant m$, such that the antecedent of I_m holds for these words, i.e.,

$$a_1 \cdot b_1 \cdot b_1^{-1} \cdot c_1 = a_2 \cdot c_2,$$

$$a_2 \cdot b_2 \cdot b_2^{-1} \cdot c_2 = a_3 \cdot c_3,$$

$$\dots\dots\dots\dots$$

$$a_m \cdot b_m \cdot b_m^{-1} \cdot c_m = a_1 \cdot c_1,$$

but

$$a_1 \cdot c_1 \neq a_2 \cdot c_2.$$

Actually we are given the equalities

$$\begin{aligned} \overline{a_1 b_1 b_1^{-1} c_1} &= \overline{a_2 c_2}, \\ \overline{a_2 b_2 b_2^{-1} c_2} &= \overline{a_3 c_3}, \\ &\cdots\cdots\cdots\cdots \\ \overline{a_m b_m b_m^{-1} c_m} &= \overline{a_1 c_1} \end{aligned} \tag{8}$$

and the inequality $\overline{a_1 c_1} \neq \overline{a_2 c_2}$.

If b_i is empty for some i, then the ith line of (8) has the form $\overline{a_i c_i} = \overline{a_{i+1} c_{i+1}}$, and we can simply skip it replacing $\overline{a_i c_i}$ in the right-hand side of the $(i-1)$st line by $\overline{a_{i+1} c_{i+1}}$. This contradicts the minimality of m. Therefore no b_i is empty.

If a is a word, we denote its length by $|a|$. Thus the length of the empty word is 0. Let $x(a)$ denote the number of occurrences of x_i and x_i^{-1} (for all possible i) in a, while $z(a)$ is the number of occurrences of z_i and z_i^{-1} in a. For example, $z(x_3 z_1^{-1} z_2 y_2 z_2^{-1}) = 3$.

Lemma 1. *$x(\overline{a_1 c_1}) = x(\overline{a_2 c_2}) = \cdots = x(\overline{a_m c_m})$ and $z(\overline{a_1 c_1}) = z(\overline{a_2 c_2}) = \cdots = z(\overline{a_m c_m})$.*

Proof. Clearly $x(\overline{ac}) \leqslant x(\overline{abb^{-1}c})$ for any words. Indeed, $x(a) = x(\bar{a})$ for every word a, because applying the defining relations of S_n to a can only change the indices of letters x_i, x_i^{-1} occurring in a, without eliminating the letters themselves. Also, obviously $x(ac) \leqslant x(abb^{-1}c)$ for any words a, b, c. Therefore $x(\overline{ac}) = x(ac) \leqslant x(abb^{-1}c) = x(\overline{abb^{-1}c})$. Applying this simple inequality to (8) we obtain $x(\overline{a_1 c_1}) \leqslant x(\overline{a_1 b_1 b_1^{-1} c_1}) = x(\overline{a_2 c_2}) \leqslant x(\overline{a_2 b_2 b_2^{-1} c_2}) = x(\overline{a_3 c_3}) \leqslant \cdots = x(\overline{a_m c_m}) \leqslant x(\overline{a_m b_m b_m^{-1} c_m}) = x(\overline{a_1 c_1})$. Therefore, $x(\overline{a_1 c_1}) \leqslant x(\overline{a_2 c_2}) \leqslant x(\overline{a_m c_m}) \leqslant x(\overline{a_1 c_1})$. Hence the first part of Lemma 1 holds. The second part of Lemma 1 may be proved analogously.

Corollary. *The words $b_1, b_2, \ldots, b_m$ have no occurrences of letters $x_i, x_i^{-1}, z_i, z_i^{-1}$, $1 \leqslant i \leqslant n+1$.*

Proof. Suppose that b_k has an occurrence of x_i or of x_i^{-1}. Then $x(\overline{a_k c_k}) < x(\overline{a_k b_k b_k^{-1} c_k}) = x(\overline{a_{k+1} b_{k+1}})$, which contradicts Lemma 1. If b_k contains z_i or z_i^{-1}, we arrive at an analogous contradiction of $z(\overline{a_k c_k}) < z(\overline{a_{k+1} b_{k+1}})$. Here the indices are considered $\operatorname{mod} m$, i.e., $a_{m+1} = a_1$, $c_{m+1} = c_1$.

The corollary is proved.

Thus, the only letters which may occur in b_j, $1 \leqslant j \leqslant m$, are y_i and y_i^{-1} for $1 \leqslant i \leqslant n+1$. If $a_j \cdot b_j \cdot b_j^{-1} \cdot c_j = a_j b_j b_j^{-1} c_j$, then $|\overline{a_{j+1} c_{j+1}}| = |\overline{a_j b_j b_j^{-1} c_j}| =$

$|a_j b_j b_j^{-1} c_j| > |a_j c_j| \geqslant |\overline{a_j c_j}|$. The inequality $a_j \cdot b_j \cdot b_j^{-1} \cdot c_j \neq a_j b_j b_j^{-1} c_j$ can hold in two cases only:

Case 1. $a_j = a_j' x_i$, $b_j = y_i$, $c_j = z_i c_j'$. In this case $\overline{a_j c_j} = \overline{a_j' x_i z_i c_j'} = a_j' x_i z_i c_j' = a_j c_j$ and $\overline{a_{j+1} c_{j+1}} = \overline{a_j b_j b_j^{-1} c_j} = \overline{a_j' x_i y_i y_i^{-1} z_i c_j'} = a_j' x_{i+1} z_{i+1} c_j'$. Hence, $|\overline{a_{j+1} c_{j+1}}| = |a_j' x_{i+1} z_{i+1} c_j'| = |a_j c_j| = |\overline{a_j c_j}|$.

Case 2. $a_j = a_j' z_i^{-1}$, $b_j = y_i$, $c_j = x_i^{-1} c_j'$. As in Case 1, we obtain $\overline{a_{j+1} c_{j+1}} = a_j' z_{i+1}^{-1} x_{i+1}^{-1} c_j'$ and $|\overline{a_{j+1} c_{j+1}}| = |\overline{a_j c_j}|$.

Thus, $|\overline{a_{j+1} c_{j+1}}| \geqslant |\overline{a_j c_j}|$ for all j. For $j = m$ we have $|\overline{a_1 c_1}| \geqslant |\overline{a_m c_m}|$. It follows that $|\overline{a_1 c_1}| \geqslant |\overline{a_m c_m}| \geqslant |\overline{a_{m-1} c_{m-1}}| \geqslant \cdots \geqslant |\overline{a_2 c_2}| \geqslant |\overline{a_1 c_1}|$. Therefore, $|\overline{a_1 c_1}| = |\overline{a_2 c_2}| = \cdots = |\overline{a_m c_m}|$, i.e., Case 1 or Case 2 holds for every $j = 1, \ldots, m$.

Thus, $\overline{a_j c_j} = a_j c_j$ for all j, and $a_{j+1} c_{j+1}$ is obtained from $a_j c_j$ in the following way: an occurrence of a subword $x_i z_i$ (or $z_i^{-1} x_i^{-1}$) in $a_j c_j$ is replaced by $x_{i+1} z_{i+1}$ (or by $z_{i+1}^{-1} x_{i+1}^{-1}$, respectively). Of course, if $i = n+1$, we assume here that $x_{i+1} = x_1$, $y_{i+1} = y_1$, $z_{i+1} = z_1$.

Now consider the transitions $a_1 c_1 \to a_2 c_2 \to \cdots \to a_m c_m \to a_1 c_1$. Under the transition $a_1 c_1 \to a_2 c_2$ a subword $x_i z_i$ [or $z_i^{-1} x_i^{-1}$] of $a_1 c_1$ is replaced by $x_{i+1} z_{i+1}$ [or $z_{i+1}^{-1} x_{i+1}^{-1}$, respectively]. Under the transition $a_2 c_2 \to a_3 c_3$ this occurrence of $x_{i+1} z_{i+1}$ [or $z_{i+1}^{-1} x_{i+1}^{-1}$] either remains unchanged or is replaced by $x_{i+2} z_{i+2}$ [or $z_{i+2}^{-1} x_{i+2}^{-1}$]. Going on to the transition $a_{m-1} c_{m-1} \to a_m c_m$ and then to $a_m c_m \to a_1 c_1$, we see that the initial occurrence of $x_i z_i$ [or $z_i^{-1} x_i^{-1}$] in $a_1 c_1$ will be replaced after m transitions by an occurrence of $x_{i+k} z_{i+k}$ [or $z_{i+k}^{-1} x_{i+k}^{-1}$] with $k \leqslant m$. However, $x_{i+k} z_{i+k} \neq x_i z_i$ [and $z_{i+k}^{-1} x_{i+k}^{-1} \neq z_i^{-1} x_i^{-1}$], which shows that we can never get back to $a_1 c_1$ after $m \leqslant n$ transitions. This contradiction shows that our original assumption—I_m fails in S_n—was erroneous. In fact, we have shown that if (8) holds in S_n then $b_1, b_2, \ldots, b_m$ are empty words, in which case, of course, $a_1 c_1 = a_2 c_2 = \cdots = a_m c_m$. Thus, S_n satisfies the axioms I_i with $i \leqslant n$.

LEMMA 2. *The infinite system of involutive semigroup axioms $I_\omega = \{I_2, I_3, \ldots\}$ is not equivalent to any of its finite subsystems.*

Proof. Consider an arbitrary finite subsystem $\{I_i, I_j, \ldots, I_n\}$, $i < j < \cdots < n$, of I_ω. The semigroup S_n satisfies all the axioms of the subsystem but it does not satisfy I_{n+1}, thus it does not satisfy the system I_ω. The statement of Lemma 2 follows.

Now we can complete our proof of Theorem 4. Suppose B is a finite system of elementary axioms for the class of all multigroups. As we know from Theorem 2, I_ω, together with the axioms defining involutive semigroups, is another system of axioms for multigroups. Thus, the two systems of axioms have precisely the same models. It follows from the

Completeness Theorem for the first-order predicate calculus (see, for example, [6, p. 73]) that every axiom from B may be formally deduced as a theorem from the axioms of the other system of axioms. Since B is finite and any formal deduction has finite length, we can use only a finite subsystem C of axioms of the other system of axioms in our deduction. Thus, B can be deduced from C. On the other hand, every axiom from the other system of axioms can be deduced from B. Thus, I_ω may be deduced in the class of involuted semigroups from a finite subsystem C of I_ω, which contradicts Lemma 2. It follows that B cannot be finite, and that completes the proof of Theorem 4.

However, in the commutative case the situation is different.

An involutive semigroup $(S; \cdot, ^{-1})$ is called *commutative* if the semigroup $(S; \cdot)$ is commutative.

THEOREM 5. *The following conditions are equivalent for a commutative involutive semigroup* $(S; \cdot, ^{-1})$:

(1) $(S; \cdot, ^{-1})$ *is a multigroup*;

(2) $(S; \cdot, ^{-1})$ *is isomorphic to an involutive semigroup of binary relations*;

(3) $(S; \cdot, ^{-1})$ *satisfies the quasi-identity*

$$x = xy^{-1}yz^{-1}z \Rightarrow x = xy^{-1}y.$$

Proof. (1)$\Rightarrow$(2). If $(S; \cdot, ^{-1})$ is a multigroup, it is isomorphic to an involutive semigroup of multipermutations. Each multipermutation is a special case of binary relation.

(2)$\Rightarrow$(3). Without loss of generality assume that $(S; \cdot, ^{-1})$ is an involutive semigroup of binary relations on a set A. Let $x = x \circ y^{-1} \circ y \circ z^{-1} \circ z$ for some $x, y, z \in S$.

Let $pr_2 x = \{b \in A: (\exists a \in A)\ [(a, b) \in x]\}$. Using commutativity we obtain $pr_2 x = pr_2 z \circ z^{-1} \circ y \circ y^{-1} \circ x \subset pr_2 z$. Analogously, using commutativity, we obtain $pr_2 x = pr_2 y \circ y^{-1} \circ z \circ z^{-1} \circ x \subset pr_2 y$. Let $\Delta_{pr_2\rho} = \{(a, a): a \in pr_2 \rho)$. Then $\Delta_{pr_2\rho} \subset \rho \circ \rho^{-1}$ for any binary relation ρ. It follows that $x = \Delta_{pr_2 x} \circ x \subset \Delta_{pr_2 y} \circ x \subset y \circ y^{-1} \circ x \subset y \circ y^{-1} \circ \Delta_{pr_2 x} \circ x \subset y \circ y^{-1} \circ \Delta_{pr_2 z} \circ x \subset y \circ y^{-1} \circ z \circ z^{-1} \circ x = x$. Therefore $x = y \circ y^{-1} \circ x = x \circ y^{-1} \circ y$ and (3) holds.

(3)$\Rightarrow$(1). Suppose that the antecedent of I_n holds. Using commutativity and denoting $x_i z_i$ by u_i, we obtain $u_1 y_1 y_1^{-1} = u_2$, $u_2 y_2 y_2^{-1} = u_3, \ldots, u_n y_n y_n^{-1} = u_1$. Therefore $u_1 y_1 y_2 y_2^{-1} \cdots y_n y_n^{-1} = u_1$, or, equivalently, $u_1 = u_1 (y_1 y_2 \cdots y_{n-1})^{-1} (y_1 y_2 \cdots y_{n-1}) y_n^{-1} y_n$. Applying (3) we obtain $u_1 = u_1 (y_1 y_2 \cdots y_{n-1})^{-1} (y_1 y_2 \cdots y_{n-1})$, i.e., $u_1 = u_1 y_1 y_1^{-1} y_2 y_2^{-1} \cdots y_{n-1} y_{n-1}^{-1}$.

Applying (3) once more, we obtain $u_1 = u_1 y_1 y_1^{-1} \cdots y_{n-2} y_{n-2}^{-1}$. Applying (3) a few times we obtain $u_1 = u_1 y_1 y_1^{-1}$, i.e., $x_1 z_1 = x_1 z_1 y_1 y_1^{-1} = x_2 z_2$. Thus, $(S; \cdot, ^{-1})$ satisfies I_n for all n, and by Theorem 2, $(S; \cdot, ^{-1})$ is a multigroup, i.e., (1) holds.

3. Multigroups with Inverting Involution

The involution operation $^{-1}$ of involutive semigroup $(S; \cdot, ^{-1})$ is called *inverting* if, for every $s \in S$, the element s^{-1} is an inverse of s, i.e., if $(S; \cdot, ^{-1})$ satisfies the identity

$$xx^{-1}x = x. \tag{9}$$

THEOREM 6. *A multigroup has an inverting involution if and only if it is an inverse semigroup.*

Proof. Necessity. Suppose that $(S; \cdot, ^{-1})$ is a multigroup with an inverting involution. Then there exists an order relation $\leqslant$ on S such that $(S; \cdot, ^{-1}, \leqslant)$ satisfies all conditions of Theorem 1. By (3), $x^{-1}x \leqslant xx^{-1}x^{-1}x$ and $xx^{-1} \leqslant x^{-1}xxx^{-1}$. Applying the involution to the latter inequality we obtain $xx^{-1} \leqslant xx^{-1}x^{-1}x$. Therefore, $x^{-1}x \cdot xx^{-1} \leqslant xx^{-1}x^{-1}x \cdot xx^{-1}x^{-1}x = x(x^2)^{-1}x^2(x^2)^{-1}x = x(x^2(x^2)^{-1}x^2)^{-1}x = x(x^2)^{-1}x = xx^{-1}x^{-1}x$. Interchanging x and x^{-1} we obtain $xx^{-1}x^{-1}x \leqslant x^{-1}xxx^{-1}$; hence identities (1) hold, i.e., $(S; \cdot, ^{-1})$ is an inverse semigroup.

Conversely, suppose that $(S; \cdot, ^{-1})$ is an inverse semigroup. By (1), it is an involutive semigroup with an inverting involution. It remains to prove that it is a multigroup. Let $\leqslant$ denote the natural order relation on $(S; \cdot, ^{-1})$. Then $\leqslant$ is stable both under multiplication $\cdot$ and involution $^{-1}$. Moreover, $yy^{-1}x \leqslant x$ for all $x, y \in S$. Thus, $(S; \cdot, ^{-1}, \geqslant)$ satisfies all conditions of Theorem 1. It follows from Theorem 1 that $(S; \cdot, ^{-1})$ is isomorphic to an involutive semigroup of multipermutations, i.e., that $(S; \cdot, ^{-1})$ is a multigroup. This completes the proof of Theorem 6. A straightforward proof of this theorem is given in [18].

COROLLARY. *Every inverse semigroup is a multigroup.*

A binary relation ρ is called *difunctional* if $\rho \circ \rho^{-1} \circ \rho \subset \rho$. Since $\rho \subset \rho \circ \rho^{-1} \circ \rho$ holds for every binary relation ρ, the former inclusion is equivalent to the condition $\rho \circ \rho^{-1} \circ \rho = \rho$. There exist many equivalent characterizations of difunctional binary relations (see [11, 12]). For example, if $\rho\langle a \rangle = \{b: (a, b) \in \rho\}$ denotes the set of all images of a under ρ, and $\rho^{-1}\langle b \rangle = \{a: (a, b) \in \rho\}$ is the set of all inverse images of b under ρ, then ρ

is difunctional if and only if any of the following equivalent conditions holds:

$$\rho\langle a_1\rangle\cap\rho\langle a_2\rangle\neq\varnothing\Rightarrow\rho\langle a_1\rangle=\rho\langle a_2\rangle,$$
$$\rho^{-1}\langle b_1\rangle\cap\rho^{-1}\langle b_2\rangle\neq\varnothing\Rightarrow\rho^{-1}\langle b_1\rangle=\rho^{-1}\langle b_2\rangle.$$

Clearly, every transformation or partial transformation of a set is a difunctional binary relation.

As it follows from the definition, if ρ is a difunctional binary relation, then ρ^{-1} is a difunctional binary relation which is an inverse for ρ, i.e., $\rho\circ\rho^{-1}\circ\rho=\rho$ and $\rho^{-1}\circ\rho\circ\rho^{-1}=\rho^{-1}$. Conversely, if ρ and σ are difunctional multipermutations of a set A and σ is an inverse for ρ in the semigroup B_A of all binary relations on A, then $\sigma=\rho^{-1}$. This fact is proved in [18, Proposition 5].

Theorem 7 produces a completely new representation theorem for inverse semigroups which is alternative to the Wagner–Preston Representation Theorem:

THEOREM 7. *Every involutive semigroup $(\Phi;\circ,^{-1})$ of difunctional multipermutations is an inverse semigroup. Conversely, every inverse semigroup $(S;\cdot,^{-1})$ is isomorphic to an involutive semigroup of difunctional multipermutations.*

Proof. If $(\Phi;\circ,^{-1})$ consists of difunctional multipermutations, then it is a multigroup satisfying the identity (9). By Theorem 6 it is an inverse semigroup. Conversely, by Theorem 6, every inverse semigroup is isomorphic to an involutive semigroup $(\Phi;\circ,^{-1})$ of multipermutations with an inverting involution. All elements of Φ are difunctional because they satisfy (9).

Inverse semigroups can be represented either by one-to-one partial transformations or by difunctional multipermutations. Which sort of representation is "better" depends mainly on psychological preferences. Now, after more than 30 years of development of the theory of inverse semigroups, their representations by one-to-one partial transformations seem to be the most natural thing in the world. However, even a brief look at the history of the concept of inverse semigroups—as developed in geometry from S. Lie and E. Cartan to V. V. Wagner—shows that the concept of the product of partial transformations, as understood now, evaded quite a few of the best minds for long years. Our present perceptions may be—at least partly—a matter of habit.

What about difunctional relations? Are they not an exotic and artificial object, much less natural than one-to-one partial transformations? In fact, difunctional relations are a very natural object in a group or group-like context.

Suppose A and B are mathematical structures, say universal algebras belonging to a variety V of algebras. The concept of isomorphism of A and B is one of the fundamental and deep concepts of mathematics. This concept permits various generalizations—at least as many as those of the concept of permutation. The most obvious generalization is that of homomorphism. Going further, we may assume that not every element of A has an image under a homomorphism, i.e., some elements of A have 0 images. Thus we arrive at a concept of local (or partial) isomorphisms and homomorphisms.

Of course, the next step is now obvious: What if different elements of A have different numbers of homomorphic (or isomorphic) images, not necessarily 0 or 1? We can naturally define "multihomomorphisms." For the sake of simplicity, assume that A and B are groupoids (sets with a binary multiplication). A multihomomorphism of A into B is a multivalued mapping ϕ of A into B which "preserves the multiplication" in the sense that, if $a_1, a_2 \in A$ and if b_1 is one of the images of a_1 under ϕ and b_2 is one of the images a_2, then $b_1 b_2$ is one of the images of $a_1 a_2$ under ϕ. The closest thing to "multi-isomorphisms" is a multihomomorphism ϕ such that each element of A has at least one image under ϕ and each element of B has at least one inverse image under ϕ. Thus, instead of groups of automorphisms of an algebra we can consider "generalized groups" of "multi-automorphisms." It turns out that, for a vast variety of mathematical structures, "multi-automorphisms" (and "multihomomorphisms") are difunctional, so that, by our Theorem 7, "generalized groups of multi-automorphisms" are always inverse semigroups! In fact, that happens each time when congruences on each algebra $A \in V$ commute. Anyone acquainted with universal algebra can easily prove that the following conditions are equivalent:

(1) Congruences on each algebra $A \in V$ commute;

(2) For any $A \in V$ the set of all multi-automorphisms of A is an inverse semigroup.

For example, if A is a group, a ring, a Boolean algebra, a vector space over a field, or even a module over a ring, then all multi-automorphisms of A form an inverse semigroup!

If $A = (A; \cdot, ^{-1})$ is a group, then a multi-automorphism of A is any multipermutation ϕ of A such that $(a_1, b_1) \in \phi$ & $(a_2, b_2) \in \phi \Rightarrow (a_1 a_2, b_1 b_2) \in \phi$ and $(a, b) \in \phi \Rightarrow (a^{-1}, b^{-1}) \in \phi$ for all $a, a_1, a_2, b, b_1, b_2 \in A$.

Suppose that $(a, b) \in \phi \circ \phi^{-1} \circ \phi$, i.e., $(a, b_1) \in \phi$, $(b_1, a_1) \in \phi^{-1}$, and $(a_1, b) \in \phi$ for some $a_1, b_1 \in A$. Then $(a_1, b_1) \in \phi$, hence $(a_1^{-1}, b_1^{-1}) \in \phi$. It follows that $(a, b) = (aa_1^{-1}a_1, b_1b_1^{-1}b) \in \phi$, i.e., $\phi \circ \phi^{-1} \circ \phi \subset \phi$ and ϕ is difunctional. The set of all multi-automorphisms of A is obviously closed under multiplication and involution: if ϕ and ψ are multi-automorphisms, then so are $\psi \circ \phi$ and ϕ^{-1}. By Theorem 7, the multigroup of all multi-automorphisms of A is an inverse semigroup.

For a duscussion of "multihomomorphisms" of modules over a ring and their importance in homological algebra and other applications, see [7]. Of course, the multihomomorphisms of modules are difunctional and so Theorem 7 can be applied in this situation as well.

The inverse semigroup of all multi-automorphisms of a group is quite a powerful structure. Already the first attempts of studying it produce spectacular results. For example, a former student of the author proved in his Ph.D. dissertation [2] that if A is an abelian group and B a group, then the inverse semigroups of multi-automorphisms of A and B are isomorphic if and only if A and B are isomorphic.

Since multi-automorphisms of a vector space form an inverse semigroup, this inverse semigroup is an analog and generalization of the full linear group (i.e., of the group of all automorphisms of a vector space). Thus, one can consider linear representations of inverse semigroups (i.e., homomorphisms into the inverse semigroups of all multi-automorphisms of a linear space), and they are natural analogs of linear representations of groups. Some of these possibilities were briefly mentioned in [19, pp. 32–34].

Next, we mention without proof some results from [17, 18]. As we have seen, if Φ is a regular semigroup of difunctional multipermutations, then it is an inverse semigroup and inverses for the elements of Φ are just the inverse (= converse) multipermutations. It is easy to see that the idempotents of Φ are precisely all equivalence relations belonging to Φ. Thus, another corollary to Theorem 7 states that every semilattice (i.e., a commutative idempotent semigroup) is isomorphic to a semigroup of equivalence relations and, conversely, every semigroup of equivalence relations is a semilattice.

The natural (or, as Wagner called it, "canonical") order relation $\leqslant$ is very important for inverse semigroups. If $(\Phi, \circ)$ is an inverse semigroup of difunctional multipermutations, then the natural order relation on Φ coincides with the converse of the set-theoretical inclusion relation, i.e., $\phi \leqslant \psi \Leftrightarrow \phi \supset \psi$ for all $\phi, \psi \in \Phi$.

In contradistinction to one-to-one partial transformations, a product of two difunctional multipermutations need not be difunctional. Thus, there is no such thing as the inverse semigroup of *all* difunctional multipermutations of a set (however, *all* multi-automorphisms of a group, a vector space, etc., do form an inverse semigroup). A description of all maximal inverse semigroups of difunctional multipermutations of a set and classification (up to isomorphism) of such inverse semigroups may be an interesting problem. Another interesting problem is a description of all isomorphic (or homomorphic) representations of an abstract inverse semigroup by difunctional multipermutations. An analogous problem for representations by one-to-one partial transformations was solved in [14].

A semigroup S is said to be *embeddable* in an involutive semigroup $(T; \cdot, ^{-1})$ if S is embeddable in the semigroup $(T; \cdot)$.

It was proved in [16] that every semigroup is isomorphic to a semigroup of multipermutations on a set. It follows that *every semigroup is embeddable in a multigroup.*

Obviously, a semigroup is isomorphic to a semigroup of permutations [one-to-one partial transformations] if and only if it is embeddable in a group [inverse semigroup]. What about difunctional multipermutations? If a semigroup S is embeddable in an inverse semigroup T, then S is isomorphic to a semigroup of difunctional multipermutation (to prove this apply Theorem 7 to T). However, the converse is not obvious. In [18] there is an example of a semigroup S of difunctional multipermutations of a set A with five elements such that S is not a subsemigroup of any inverse semigroup of difunctional multipermutations of A. However, using a criterion of embeddability of a semigroup in an inverse semigroup from [13] we were able to prove in [18, Theorem 13] that every semigroup of difunctional multipermutations is embeddable in an inverse semigroup. Thus, *a semigroup is isomorphic to a semigroup of difunctional multipermutations if and only if it is embeddable in an inverse semigroup.*

Acknowledgments

This paper was written in 1977 in Russian and submitted to a Soviet mathematical journal in January 1978. It had been accepted for publication but, in the fall of 1979, when I was about to leave the USSR, the manuscript was returned to me by the publisher without any explanations. I was not allowed to take it with me or to mail it abroad. It took five years and the efforts of four mathematicians from four countries to rescue the manuscript. I am very grateful to all of them, and I am sorry that I cannot give their names here without hurting some of them.

This paper is a slightly changed translation of the original Russian manuscript.

References

1. D. A. Bredikhin, Representation of ordered involuted semigroups, *Izv. Vyssh. Uchebn. Zaved. Mat.*, 1975, no. 7, 19–29. [Russian]
2. D. A. Bredikhin, "Multiplicative Algebras of Relations," Dissertation, Saratov State University, Saratov, USSR, 1976. [Russian]
3. B. Jónsson, Representation of modular lattices and relation algebras, *Trans. Amer. Math. Soc.* **92** (1959), 449–464.

4. R. C. LYNDON, The representation of relational algebras, *Ann. of Math.* **51** (1950), 707–729.
5. R. C. LYNDON, The representation of relation algebras, II, *Ann. of Math.* **63** (1956), 294–307.
6. R. C. LYNDON, "Notes on Logic," Van Nostrand, Princeton, NJ, 1966.
7. S. MACLANE, An algebra of additive relations, *Proc. Nat. Acad. Sci. U.S.A.* **47**, No. 7 (1961), 1043–1051.
8. L. NOVÝ, "Origins of Modern Algebra," Noordhoff, Leyden, 1973.
9. G. B. PRESTON, Inverse semi-groups, *J. London Math. Soc.* **29** (1954), 396–403.
10. G. B. PRESTON, Representations of inverse semigroups, *J. London Math. Soc.* **29** (1954), 411–419.
11. J. RIGUET, Relations binaires, fermetures, correspondances de Galois, *Bull. Soc. Math. France* **76** (1948), 114–115.
12. J. RIGUET, "Fondements de la théorie des relations binaires," Thése, Paris, 1951.
13. B. M. SCHEIN [ŠAĬN], Embedding a semigroup in a generalized group, *Mat. Sb.* **55** (1961), 379–400 [Russian]; English transl.: *Amer. Math. Soc. Transl. (2)*, **39** (1987).
14. B. M. SCHEIN, Representations of generalized groups, *Izv. Vyssh. Uchebn. Zaved Mat.*, 1962, no. 3, 164–176. [Russian]
15. B. M. SCHEIN, On the theory of generalized groups, *Dokl. Akad. Nauk SSSR* **153** (1963), 296–299 [Russian]; English transl.: *Soviet Math. Dokl.* **4** (1963), 1680–1683.
16. B. M. SCHEIN, Representation of semigroups by binary relations, *Mat. Sb.* **60** (1963), 293–303. [Russian]
17. B. M. SCHEIN, Involuted semigroups of full binary relations, *Dokl. Akad. Nauk SSSR* **156** (1964), 1300–1303 [Russian]; English transl.: *Soviet Math. Dokl.* **5** (1964), 839–842.
18. B. M. SCHEIN, On certain classes of semigroups of binary relations, *Sibirsk. Mat. Zh.* **6** (1965), 616–635 [Russian]; English translation: *Amer. Math. Soc. Transl. (2)*, **139** (1987), in press.
19. B. M. SCHEIN, Relation algebras and function semigroups, *Semigroup Forum* **1** (1970), 1–62.
20. B. M. SCHEIN, A solution to the problem of representation of involuted semigroups and semigroups by binary relations, *in* "Summaries of Talks at the XII All-Union Algebraic Colloquium," Sverdlovsk, 1973, Vol. 2, 243. [Russian]
21. B. M. SCHEIN, Representation of involuted semigroups by binary relations, *Fund. Math.* **82** (1974), 121–141.
22. A. TARSKI, On the calculus of relations, *J. Symbolic Logic* **6** (1941), 73–89.
23. V. V. WAGNER [VAGNER], Generalized groups, *Dokl. Akad. Nauk SSSR* **84** (1952), 1119–1122. [Russian]
24. V. V. WAGNER, Representation of ordered semigroups, *Mat. Sb.* **38** (1956), 203–240 [Russian]; English transl.: *Amer. Math. Soc. Transl. (2)* **36** (1964), 295–336.
25. H. WUSSING, "Die Genesis des abstrakten Gruppenbegriffs, Ein Beitrag zur Entstehungsgeschichte der abstrakten Gruppentheorie," Deutsch. Verlag Wissenschaften, Berlin, 1969.